Ref. 3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-072872

(43)Date of publication of application : 12.03.2002

(51)Int.Cl. G09C 1/00

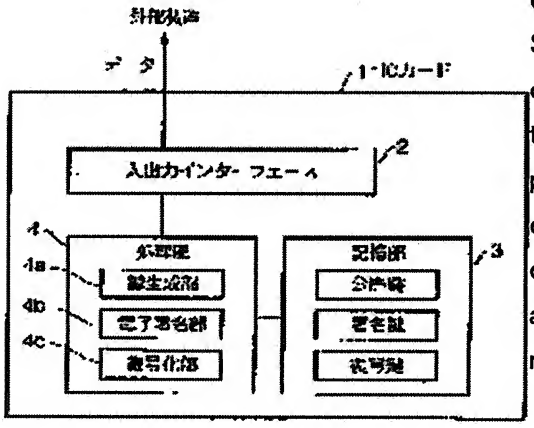
(21)Application number : 2000-259853

(22)Date of filing : 29.08.2000

(71)Applicant : NTT COMWARE CORP

(72)Inventor : FURUKAWA YOSHISATO

(54) DEVICE AND METHOD FOR SECURING DATA, AND RECORDING MEDIUM THEREOF



(57)Abstract:

PROBLEM TO BE SOLVED: To provide an enciphering system and an electronic signature system for company use.

SOLUTION: A date security device of this invention has three keys of one public key in accordance with a public key system, a signature key to be used for electronically signing a plain text together with this public key, and a decoding key for decoding the cryptogram enciphered by the public key differing from this signature key. The data security device of this invention is especially packaged as an IC, and the decoding key is separately kept by an organization for managing it.

Ref. 3

対応なし、英抄

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－72872
（P2002－72872A）
(43)公開日　平成14年３月12日(2002.3.12)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ａ　５Ｊ１０４
			６４０Ｚ
	６２０		６２０Ｂ

審査請求　有　　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－259853(P2000－259853)

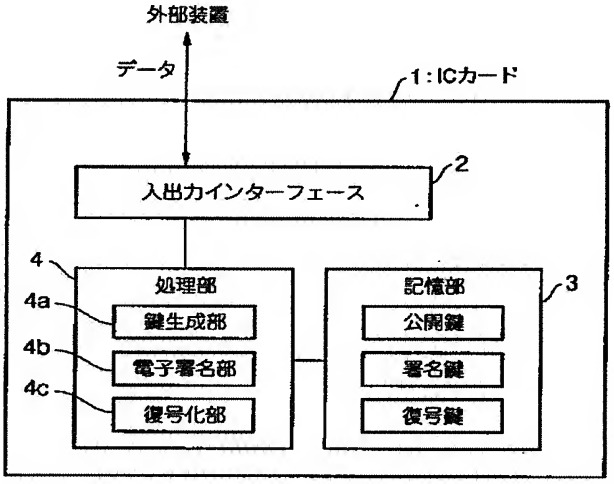
(22)出願日　平成12年８月29日(2000.8.29)

(71)出願人　397065480
エヌ・ティ・ティ・コムウェア株式会社
東京都港区港南一丁目９番１号
(72)発明者　古川　嘉識
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

Ｆターム(参考)　5J104 AA09 JA23 LA03 LA06 NA02 NA35 NA37

(54)【発明の名称】　データセキュリティ装置、データセキュリティ方法及びその記録媒体

(57)【要約】
【課題】　本発明の目的は、企業ユースにおいて、より安全な暗号方式・電子署名方式を提供することにある。
【解決手段】　本発明のデータセキュリティ装置は、公開鍵方式による、１つの公開鍵と、この公開鍵とともに利用し平文の電子署名に用いる署名鍵と、この署名鍵とは異なり公開鍵で暗号化された暗号文の復号化に用いる復号鍵の３つの鍵をもつ。本発明のデータセキュリティ装置は、特に、ＩＣカードとして実装され、復号鍵は、復号鍵を管理する機関に別途預託される。



1

【特許請求の範囲】

【請求項１】　平文の暗号化および暗号文の復号化とさらに平文の電子署名をするために用いる装置において、
前記装置は、
公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を有し、
前記第１の秘密鍵と第２の秘密鍵は異なるものであることを特徴とするデータセキュリティ装置。

【請求項２】　前記データセキュリティ装置は、
プログラム処理を行う処理部と、前記公開鍵と第１の秘密鍵と第２の秘密鍵を含むデータを記憶する記憶部と、データの入出力を行う入出力インターフェースと、を具備するＩＣカードにより構成され、
前記処理部は、
電子署名に係る暗号化を、前記記憶部に記憶された第１の秘密鍵を用いて行い、
前記公開鍵により暗号化された暗号文の復号化を、前記記憶部に記憶された第２の秘密鍵を用いて行う、
ことを特徴とする請求項１に記載のデータセキュリティ装置。

【請求項３】　前記ＩＣカードの処理部は、
前記入出力インターフェースを介して、
該ＩＣカードに接続された外部装置に、前記公開鍵を出力し、
前記外部装置から電子署名の対象となるデータが入力されると、該入力されたデータを前記第１の秘密鍵を用いて暗号化し、該暗号化により得られた暗号文を前記外部装置に出力し、
前記外部装置から前記公開鍵を用いて暗号化された暗号文が入力されると、該入力された暗号文を前記第２の秘密鍵を用いて復号化し、該復号化により得られた平文を前記外部装置に出力することを特徴とする請求項２に記載のデータセキュリティ装置。

【請求項４】　前記処理部は、
前記公開鍵と第１の秘密鍵と第２の秘密鍵を生成し前記記憶部に記憶させることを特徴とする請求項３に記載のデータセキュリティ装置。

【請求項５】　前記公開鍵方式は、
２つの相異なる素数Ｐ1およびＱ1を決定し、該Ｐ1およびＱ1に対し、（Ｐ1－１）×（Ｑ1－１）と互いに素かつＬＣＭ（Ｐ1－１，Ｑ1－１）×ｎ1＋１以外の自然数の列Ｅ1と、
前記Ｐ1およびＱ1と異なるとともに相異なる２つの素数Ｐ2およびＱ2を決定し、該Ｐ2およびＱ2に対し、（Ｐ2－１）×（Ｑ2－１）と互いに素かつＬＣＭ（Ｐ2－１，Ｑ2－１）×ｎ2＋１以外の自然数の列Ｅ2と、を求め、
前記Ｅ1およびＥ2の共通部分Ｅ1∩Ｅ2から、任意の１つの自然数Ｅを決定し、

2

ＥとＮ1＝Ｐ1×Ｑ1とＮ2＝Ｐ2×Ｑ2の組（Ｅ，Ｎ1，Ｎ2）を前記１の公開鍵とし、
等式：Ｅ×Ｄ1＝ＬＣＭ（Ｐ1－１，Ｑ1－１）×ｎ1＋１
を満たす自然数Ｄ1を決定し、Ｄ1およびＮ1の組（Ｄ1，Ｎ1）を第１の秘密鍵とし、
等式：Ｅ×Ｄ2＝ＬＣＭ（Ｐ2－１，Ｑ2－１）×ｎ2＋１
を満たす自然数Ｄ2を決定し、Ｄ2およびＮ2の組（Ｄ2，Ｎ2）を第２の秘密鍵とし、
電子署名の対象である平文に対応するデータＭ1に対し、第１の秘密鍵を用いて、その電子署名Ｓを、Ｎ1を法とし、
$S \equiv M1^{D1} \pmod{N1}$、とし、
該電子署名の確認を、公開鍵の要素であるＥとＮ1を用いて、Ｎ1を法とし、
$M1' \equiv S^{E} \pmod{N1}$、を求め、該Ｍ1'がＭ1と一致することで電子署名の確認を行い、
平文Ｍ2に対し、公開鍵の要素であるＥとＮ2を用いて、その暗号文Ｃを、Ｎ2を法とし、
$C \equiv M2^{E} \pmod{N2}$、として求め、
該暗号文Ｃの復号化を、前記第２の秘密鍵を用いて、Ｎ2を法とし、
$M2 \equiv C^{D2} \pmod{N2}$、より求めることを特徴とする請求項１ないし請求項４のいずれかに記載のデータセキュリティ装置。ただし、ＬＣＭ（Ｐ1－１，Ｑ1－１）は、（Ｐ1－１）と（Ｑ1－１）の最小公倍数であり、ＬＣＭ（Ｐ2－１，Ｑ2－１）は、（Ｐ2－１）と（Ｑ2－１）の最小公倍数であり、ｎ1およびｎ2は任意の負でない整数である。

【請求項６】　公開鍵の電子証明書において、前記公開鍵の第２要素Ｎ1と第３要素Ｎ2の一方を、ＩＴＵ－ＴＸ．５０９バージョン３の拡張領域に格納することを特徴とする請求項５に記載のデータセキュリティ装置。

【請求項７】　デジタルデータの安全を守るための方法において、
公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、さらに、該第１の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を用い、
平文の電子署名を、前記第２の秘密鍵を用いて行い、
前記公開鍵により暗号化された暗号文の復号化を、前記第１の秘密鍵を用いて行うことを特徴とするデータセキュリティ方法。

【請求項８】　請求項７に記載のデータセキュリティ方法において、
前記第２の秘密鍵を、該第２の秘密鍵を管理する鍵管理機関に預託し、
該第２の秘密鍵の所有者または該所有者より指定された者は、必要に応じて、該第２の秘密鍵を前記鍵管理機関より再取得可能とすることを特徴とするデータセキュリティ方法。

【請求項９】　プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項１に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、
公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し前記第１の秘密鍵とは異なり平文の電子署名に用いる第１の秘密鍵と、さらに、前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、からなるデータと、
平文の電子署名に係る暗号化を、前記第１の秘密鍵を用いて行う手順と、
前記公開鍵により暗号化された暗号文の復号化を、前記第２の秘密鍵を用いて行う手順と、
をコンピュータに実行させるためのプログラムを記録した記録媒体。
【請求項１０】　プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項１に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、
公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、さらに、前記第１の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を生成する手順と、
平文の電子署名に係る暗号化を、前記第１の秘密鍵を用いて行う手順と、
前記公開鍵により暗号化された暗号文の復号化を、前記第２の秘密鍵を用いて行う手順と、
をコンピュータに実行させるためのプログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルデータのセキュリティに係る暗号化および復号化ならびに電子署名に用いる装置および方法に関する。
【０００２】
【従来の技術】従来の公開鍵暗号方式では、公開鍵と秘密鍵の２つの鍵を利用し、暗号化・復号化ならびに電子署名を実現している。
【０００３】
【発明が解決しようとする課題】この公開鍵暗号方式では、公開鍵で暗号化された情報は秘密鍵でのみ復号化できる。もしこの秘密鍵を紛失してしまった場合、暗号化された情報は復号不可能となり失われてしまう。そのため企業ユースでは、社員の秘密鍵を預託という形で管理することが考えられている。一方、電子署名は、上記のように、秘密鍵で署名（暗号化）を行い、公開鍵で署名の確認を行うものである。この電子署名は、署名を行った人物しか秘密鍵を知らない原則に基づいている。つまり秘密鍵の紛失に備えて預託を行えば電子署名に係る事後否認防止性が弱まり、事後否認防止のため秘密鍵を個人管理にすれば上記のように秘密鍵紛失と同時に情報を失う危険性が発生する（図６参照）。以上のように、従来の２つの鍵を用いた公開鍵暗号方式による、暗号化復号化および電子署名は、必ずしも安全なものとは言えない。

【０００４】本発明は、上記の点に鑑みてなされたもので、企業ユースにおいて、より安全な暗号方式・電子署名方式を提供するものである。
【０００５】
【課題を解決するための手段】本発明のデータセキュリティ装置は、平文の暗号化および暗号文の復号化とさらに平文の電子署名をするために用いる装置において、前記装置は、公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を有し、前記第１の秘密鍵と第２の秘密鍵は異なるものであることを特徴とする。
【０００６】また、本発明のデータセキュリティ装置は、プログラム処理を行う処理部と、前記公開鍵と第１の秘密鍵と第２の秘密鍵を含むデータを記憶する記憶部と、データの入出力を行う入出力インターフェースと、を具備するＩＣカードにより構成され、前記処理部は、電子署名に係る暗号化を、前記記憶部に記憶された第１の秘密鍵を用いて行い、前記公開鍵により暗号化された暗号文の復号化を、前記記憶部に記憶された第２の秘密鍵を用いて行う、ことを特徴とする。
【０００７】また、本発明のデータセキュリティ装置において、前記ＩＣカードの処理部は、前記入出力インターフェースを介して、該ＩＣカードに接続された外部装置に、前記公開鍵を出力し、前記外部装置から電子署名の対象となるデータが入力されると、該入力されたデータを前記第１の秘密鍵を用いて暗号化し、該暗号化により得られた暗号文を前記外部装置に出力し、前記外部装置から前記公開鍵を用いて暗号化された暗号文が入力されると、該入力された暗号文を前記第２の秘密鍵を用いて復号化し、該復号化により得られた平文を前記外部装置に出力することを特徴とする。
【０００８】また、本発明のデータセキュリティ装置において、前記処理部は、前記公開鍵と第１の秘密鍵と第２の秘密鍵を生成し前記記憶部に記憶させることを特徴とする。
【０００９】また、本発明のデータセキュリティ装置において、前記公開鍵方式は、２つの相異なる素数Ｐ1およびＱ1を決定し、該Ｐ1およびＱ1に対し、（Ｐ1－１）×（Ｑ1－１）と互いに素かつＬＣＭ（Ｐ1－１，Ｑ1－１）×ｎ1＋１以外の自然数の列Ｅ1と、前記Ｐ1およびＱ1と異なるとともに相異なる２つの素数Ｐ2およびＱ2

を決定し、該Ｐ2およびＱ2に対し、（Ｐ2－１）×（Ｑ2－１）と互いに素かつＬＣＭ（Ｐ2－１，Ｑ2－１）×ｎ2＋１以外の自然数の列Ｅ2と、を求め、前記Ｅ1およびＥ2の共通部分Ｅ1∩Ｅ2から、任意の１つの自然数Ｅを決定し、ＥとＮ1＝Ｐ1×Ｑ1とＮ2＝Ｐ2×Ｑ2の組（Ｅ，Ｎ1，Ｎ2）を前記１の公開鍵とし、等式：Ｅ×Ｄ1＝ＬＣＭ（Ｐ1－１，Ｑ1－１）×ｎ1＋１を満たす自然数Ｄ1を決定し、Ｄ1およびＮ1の組（Ｄ1，Ｎ1）を第１の秘密鍵とし、等式：Ｅ×Ｄ2＝ＬＣＭ（Ｐ2－１，Ｑ2－１）×ｎ2＋１を満たす自然数Ｄ2を決定し、Ｄ2およびＮ2の組（Ｄ2，Ｎ2）を第２の秘密鍵とし、電子署名の対象である平文に対応するデータＭ1に対し、第１の秘密鍵を用いて、その電子署名Ｓを、Ｎ1を法とし、$S \equiv M1^{D1}$（ｍｏｄＮ1）、とし、該電子署名の確認を、公開鍵の要素であるＥとＮ1を用いて、Ｎ1を法とし、$M1' \equiv S^{E}$（ｍｏｄＮ1）、を求め、該Ｍ1'がＭ1と一致することで電子署名の確認を行い、平文Ｍ2に対し、公開鍵の要素であるＥとＮ2を用いて、その暗号文Ｃを、Ｎ2を法とし、$C \equiv M2^{E}$（ｍｏｄＮ2）、として求め、該暗号文Ｃの復号化を、前記第２の秘密鍵を用いて、Ｎ2を法とし、$M2 \equiv C^{D2}$（ｍｏｄＮ2）、より求めることを特徴とする。ただし、ＬＣＭ（Ｐ1－１，Ｑ1－１）は、（Ｐ1－１）と（Ｑ1－１）の最小公倍数であり、ＬＣＭ（Ｐ2－１，Ｑ2－１）は、（Ｐ2－１）と（Ｑ2－１）の最小公倍数であり、ｎ1およびｎ2は任意の負でない整数である。

【００１０】また、本発明は、公開鍵の電子証明書において、前記公開鍵の第２要素Ｎ1と第３要素Ｎ2の一方を、ＩＴＵ－Ｔ　Ｘ．５０９バージョン３の拡張領域に格納することを特徴とする。

【００１１】また、本発明のデータセキュリティ方法は、デジタルデータの安全を守るための方法において、公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、さらに、該第１の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を用い、平文の電子署名を、前記第２の秘密鍵を用いて行い、前記公開鍵により暗号化された暗号文の復号化を、前記第１の秘密鍵を用いて行うことを特徴とする。

【００１２】また、請求項７に記載のデータセキュリティ方法において、前記第２の秘密鍵を、該第２の秘密鍵を管理する鍵管理機関に預託し、該第２の秘密鍵の所有者または該所有者より指定された者は、必要に応じて、該第２の秘密鍵を前記鍵管理機関より再取得可能とすることを特徴とする。

【００１３】また、本発明は、プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項１に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し前記第１の秘密鍵とは異なり平文の電子署名に用いる第１の秘密鍵と、さらに、前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、からなるデータと、平文の電子署名に係る暗号化を、前記第１の秘密鍵を用いて行う手順と、前記公開鍵により暗号化された暗号文の復号化を、前記第２の秘密鍵を用いて行う手順と、をコンピュータに実行させるためのプログラムを記録した記録媒体である。

【００１４】また、本発明は、プログラム制御回路を含むコンピュータ装置にインストールすることにより、該コンピュータ装置が請求項１に記載のデータセキュリティ装置を実現する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体であって、公開鍵方式による、１の公開鍵と、該公開鍵とともに利用し平文の電子署名に用いる第１の秘密鍵と、さらに、前記第１の秘密鍵とは異なり前記公開鍵で暗号化された暗号文の復号化に用いる第２の秘密鍵と、を生成する手順と、平文の電子署名に係る暗号化を、前記第１の秘密鍵を用いて行う手順と、前記公開鍵により暗号化された暗号文の復号化を、前記第２の秘密鍵を用いて行う手順と、をコンピュータに実行させるためのプログラムを記録した記録媒体である。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態を、図面を参照して説明する。図１は、本発明の一実施の形態であるＩＣカードの構成を示すブロック図である。

【００１６】ＩＣカード１は、外部装置（図示せず）と接続されデータの入出力を行う入出力インターフェース２と、公開鍵暗号方式による公開鍵と署名鍵（第１の秘密鍵）と復号鍵（第２の秘密鍵）と一時データとを記憶する記憶部３と、下記の鍵生成部４ａと電子署名部４ｂと復号化部４ｃとからなる処理部４とから構成される。

【００１７】鍵生成部４ａは、公開鍵暗号方式による公開鍵と復号鍵と署名鍵を生成し、記憶部３に記憶させる。電子署名部４ｂは、署名鍵を用いて、電子署名のために、対象となる平文に対応するデータの暗号化をする。署名鍵を用いて暗号化されるデータの入力および暗号化されたデータの出力は、入出力インターフェース２を介して行われる。復号化部４ｃは、復号鍵を用いて、公開鍵により暗号化された暗号文を復号化する。そして、復号化した結果の平文を、入出力インターフェース２を介して外部装置に出力する。なお、この公開鍵は、入出力インターフェース２を介して外部装置に出力（提供）され、外部装置によりこの公開鍵を使って平文の暗号化がなされる。

【００１８】なお、記憶部３は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等の揮発性の記憶素子により構成されている。また、この処理部４はメモリおよびＣＰＵ（中央演算装置）等により構成され、処理部４

の各機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能が実現されるものとする。また、このプログラムは、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等の不揮発性の記憶素子（図示せず）に記憶されているものとする。

【００１９】次に、このように構成された本実施の形態のＩＣカード１の動作について、図２～４を参照して説明する。

【００２０】まず、はじめに、鍵生成部４ａは、公開鍵暗号方式に基づく公開鍵と復号鍵と署名鍵を生成し（図３：①、図４（ａ）：①）、記憶部３に記憶させる（図２：ステップＳ１）。なお、ここで生成する３つの鍵生成の具体例は後述する。次に、処理部４は、ＩＣカード１が接続された外部装置からの要求により、記憶部３から公開鍵を読み出し、入出力インターフェース２を介して外部装置へ出力する（図３：②、図４（ａ）：②、図２：ステップＳ２）。同様に、処理部４は、外部装置からの要求により、記憶部３から復号鍵を読み出し、入出力インターフェース２を介して外部装置へ出力する（図２：ステップＳ３）。

【００２１】なお、出力された公開鍵は、認証機関（ＣＡ）により証明書（Ｘ．５０９証明書）という形で、他のユーザに公開される（図３：④）。また、復号鍵は、秘密鍵を管理する所定の鍵管理機関に預託され別途管理される（図３：③、図４（ａ）：③）。一方、署名鍵は、ＩＣカード１の外部に出力されることはない。これらにより、ＩＣカード１の紛失や破壊によって復号鍵の失ったとしても、上記鍵管理機関において保管された復号鍵を用いて、対応する公開鍵により暗号化された暗号文の復号化を実施することが可能となる。また、署名鍵は、ＩＣカード１の外部に出力されることはないので、署名鍵を用いてなされた電子署名に対して、事後否認防止性が弱まることはない。

【００２２】次に、外部装置から入出力インターフェース２を介して、電子署名の対象となる平文に対応するデータと電子署名要求が、入出力インターフェース２を介して入力されると（図２：ステップＳ４）、電子署名部４ｂは、記憶部３から署名鍵を読み出し、この署名鍵を＊用いて入力された対象となる平文に対応するデータを暗号化する（図４（ｂ）：①、図２：ステップＳ５）。そして、この暗号化されたデータ（署名データ）を、入出力インターフェース２を介して外部装置に出力する（図２：ステップＳ６）。なお、他のユーザは、電子署名を行ったユーザの証明書（公開鍵を含む）と、この暗号化されたデータ（署名データ）と、平文とから署名の確認を行う（図４（ｂ）：②）。

【００２３】また、公開鍵を得た外部装置により、この公開鍵を用いて平文が暗号化され（図４（ｃ）：①）、暗号文と復号化要求が入出力インターフェース２を介して入力されると（図２：ステップＳ７）、復号化部４ｃは記憶部３から復号鍵を読み出し、入力された暗号文を復号化する（図４（ｃ）：②、図２：ステップＳ８）。そして、復号化した平文を入出力インターフェース２を介して、外部装置に出力する（図２：ステップＳ９）。なお、ユーザが復号鍵を紛失した場合、鍵管理機関に預託した復号鍵を用いて暗号文を復号化することも、預託した復号鍵をもとに復号鍵を復元することもできる（図４（ｃ）：③）。以上、ＩＣカード１の動作を説明した。なお、上記で説明した動作フローは一例であり、上記の処理の流れに限定されるものではない。

【００２４】次に、上記公開鍵と復号鍵と署名鍵の生成について、具体的実施例をあげ説明する。

【００２５】［実施例１］以下では、ＲＳＡ（Ｒｉｖｅｓｔ Ｓｈａｍｉｒ Ａｄｌｅｍａｎ）暗号方式を応用した、３つの鍵の生成例である。なお、一般に知られているＲＳＡ暗号方式の詳細については、その説明を省略する。

【００２６】まず、署名鍵のもととなる相異なる２つの素数Ｐ1とＱ1を任意に選択する。ここでは、Ｐ1＝２、Ｑ1＝５とする。次に、Ｐ1とＱ1の積であるＮ1を求める。

Ｎ1＝Ｐ1×Ｑ1＝１０

ここで、Ｎ1＝１０を法とする世界は、表１のようになる。

【表１】

P1=2, Q1=5

	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2	4	8
3	3	9	7	1	3	9	7	1	3	9	7
4	4	6	4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7	9	3
8	8	4	2	6	8	4	2	6	8	4	2
9	9	1	9	1	9	1	9	1	9	1	9

n1	4n1+1	D1
1	5	0.454545
2	9	0.818182
3	13	1.181818
4	17	1.545455
5	21	1.909091
6	25	2.272727
7	29	2.636364
8	33	3
9	37	3.363636

ED1=4n1+1
E=11, n1=8, D1=3

この表の各行は、第１列の自然数（１～９）を、１～１１までべき乗した値に対しＮ1を法とする剰余からなっている。これからも分かるように、各行はＰ1－１とＱ1－１の最小公倍数（ここでは、４）の周期性をもってい

る。

【００２７】ここで、署名鍵に対応する公開鍵の第１要素の候補となる自然数の列Ｅ1は、（Ｐ1－１）×（Ｑ1－１）と互いに素であり、かつ、４ｎ1＋１（ｎ1は、負でない整数）以外の自然数の集合として求める。ここでは、Ｅ1＝｛３，７，１１，…｝となる。

【００２８】次に、復号鍵のもととなる相異なる２つの＊素数Ｐ2とＱ2を任意に選択する。ここでは、Ｐ2＝３、Ｑ2＝７とする。次に、Ｐ2とＱ2の積であるＮ2を求める。

Ｎ2＝Ｐ2×Ｑ2＝２１

ここで、Ｎ2＝２１を法とする世界は、表２のようになる。

【表２】

P2=3, Q2=7

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	11	1	2	4	8	16	11	1	2	4	8
3	3	9	6	18	12	15	3	9	6	18	12	15	3	9	6
4	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1
5	5	4	20	16	17	1	5	4	20	16	17	1	5	4	20
6	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8
9	9	18	15	9	18	15	9	18	15	9	18	15	9	18	15
10	10	16	13	4	19	1	10	16	13	4	19	1	10	16	13
11	11	16	8	4	2	1	11	16	8	4	2	1	11	16	8
12	12	18	6	9	3	15	12	18	6	9	3	15	12	18	6
13	13	1	13	1	13	1	13	1	13	1	13	1	13	1	13
14	14	7	14	7	14	7	14	7	14	7	14	7	14	7	14
15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
16	16	4	1	16	4	1	16	4	1	16	4	1	16	4	1

n2	6n2+1	D2
1	7	0.636364
2	13	1.181818
3	19	1.727273
4	25	2.272727
5	31	2.818182
6	37	3.363636
7	43	3.909091
8	49	4.454545
9	55	5
10	61	5.545455
11	67	6.090909
12	73	6.636364
13	79	7.181818
14	85	7.727273
15	91	8.272727
16	97	8.818182

ED2=6n2+1
E=11, n2=9, D2=5

この表の各行は、第１列の自然数（１～１６）を、１～１５までべき乗した値に対しＮ2を法とする剰余からなっている。これからも分かるように、各行はＰ2－１とＱ2－１の最小公倍数（ここでは、６）の周期性をもっている。

【００２９】ここで、復号鍵に対応する公開鍵の第１要素の候補となる自然数の列Ｅ2は、（Ｐ2－１）×（Ｑ2－１）と互いに素であり、かつ、６ｎ2＋１（ｎ2は、負でない整数）以外の自然数の集合として求める。ここでは、Ｅ2＝｛５，１１，…｝となる。

【００３０】以上で得られた、２つの秘密鍵（署名鍵、復号鍵）に共通して対応する公開鍵の第１要素の候補となる自然数の列Ｅ0が、署名鍵に対応する公開鍵の第１要素の候補となる自然数の列Ｅ1と復号鍵に対応する公開鍵の第１要素の候補となる自然数の列Ｅ2の共通部分として得られる。すなわち、

Ｅ0＝Ｅ1∩Ｅ2＝｛１１，…｝

ここで、公開鍵の第１要素Ｅとして１つを決定する。ここでは、Ｅ＝１１とする。以上により、公開鍵（Ｅ，Ｎ1，Ｎ2）は、（１１，１０，２１）となる。

【００３１】次に、等式：Ｅ×Ｄ1＝ＬＣＭ（Ｐ1－１，Ｑ1－１）×ｎ1＋１を満たす自然数Ｄ1を１つ決定し、Ｄ1およびＮ1の組（Ｄ1，Ｎ1）を署名鍵（第１の秘密鍵）とする。ここでは、Ｐ1＝２、Ｑ1＝５、公開鍵の第１要素ＥをＥ＝１１としているので、上記等式を満たすＤ1＝３を用い、署名鍵を（３、１０）とする。

【００３２】次に、等式：Ｅ×Ｄ2＝ＬＣＭ（Ｐ2－１，Ｑ2－１）×ｎ2＋１を満たす自然数Ｄ2を１つ決定し、Ｄ2およびＮ2の組（Ｄ2，Ｎ2）を復号鍵（第２の秘密鍵）とする。ここでは、Ｐ2＝３、Ｑ2＝７、公開鍵の第１要素ＥをＥ＝１１としているので、上記等式を満たすＤ2＝５を用い、復号鍵を（５、２１）とする。

【００３３】次に、署名鍵（Ｄ1，Ｎ1）を用いた電子署名（署名データ）Ｓは、次式により算出される。ここでは、電子署名の対象となるデータをＭとしている。

$S \equiv M^{D1} \pmod{N1}$

そして、公開鍵（Ｅ，Ｎ1，Ｎ2）を用いて、次式によりＭ’を求め、Ｍ’とＭが一致することで署名を確認することができる。

$M' \equiv S^{E} \pmod{N1}$

【００３４】例えば、署名鍵を用い平文（２、４、６）を暗号化すると、署名（署名データ）は、以下のようになる。

平文	署名
2	$2^3 \equiv 8 \pmod{10}$
4	$4^3 \equiv 4 \pmod{10}$
6	$6^3 \equiv 6 \pmod{10}$

【００３５】これらの署名データに対し、公開鍵（１１，１０，２１）を用いて、署名データを復号化すると、

署名	平文
8	$8^{11} \equiv 2 \pmod{10}$
4	$4^{11} \equiv 4 \pmod{10}$
6	$6^{11} \equiv 6 \pmod{10}$

となる。

【００３６】このように、署名鍵（Ｄ1，Ｎ1）＝（３、１０）を用いて暗号化された署名データは、公開鍵（Ｅ，Ｎ1，Ｎ2）＝（１１，１０，２１）を用いて復号化できる。そして、署名データから公開鍵（Ｅ，Ｎ1，Ｎ2）を用いてもとの平文が得られることで、確かに公開鍵を公開した者による平文とその署名であることが確認できる。上記例で、Ｍとして平文のデータを用いてい

るが、例えば、電子署名の対象となる平文を、ハッシュ関数を用いて変換したものを用いてもよい。

【００３７】次に、公開鍵（Ｅ，Ｎ1，Ｎ2）を用いた平文Ｍの暗号化は、次式により行われる。

$C \equiv M^{E} \pmod{N2}$

そして、復号鍵（Ｄ2，Ｎ2）を用いて、次式により復号化が行われる。

$M \equiv C^{D2} \pmod{N2}$

【００３８】例えば、公開鍵を取得した者が、この公開鍵を用いて平文（２、４、６）を暗号化すると、以下のようになる。

平文	暗号文
2	$2^{11} \pmod{21} \equiv 11$
4	$4^{11} \pmod{21} \equiv 16$
6	$6^{11} \pmod{21} \equiv 6$

【００３９】そして、この暗号文は、復号鍵を用いて以下のように復号化される。

暗号文	平文
11	$11^{5} \pmod{21} \equiv 2$
16	$16^{5} \pmod{21} \equiv 4$
6	$6^{5} \pmod{21} \equiv 6$

【００４０】このように、公開鍵（Ｅ，Ｎ1，Ｎ2）＝（１１，１０，２１）用いて暗号化された暗号文は、復号鍵（Ｄ2，Ｎ2）＝（５、２１）を用いて復号化できる。以上のようにして、１つの公開鍵と、署名鍵と、復号鍵とを生成することができる。

【００４１】従来のＲＳＡ暗号方式では、上記で説明した（Ｅ，Ｎ1）の組で署名鍵に対応する公開鍵をなし、また、（Ｅ，Ｎ2）の組で復号鍵に対応する公開鍵をなすが、本実施例では、（Ｅ，Ｎ1，Ｎ2）の組で１つの公開鍵を構成している。こうすることで、２つの公開鍵（Ｅ，Ｎ1）および（Ｅ，Ｎ2）を用いるよりも、鍵のデータ長を短くすることができる。また、公開鍵を２つ管理する必要がなくなる。

【００４２】［実施例２］以下では、Ｅ１Ｇａｍａ１暗号方式を応用した、３つの鍵の生成例である。なお、一般に知られているＥ１Ｇａｍａ１暗号方式の詳細については、その説明を省略する。

【００４３】本実施例で用いる、１つの公開鍵（ｇ，ｐ，Ｔ1，Ｔ2）と、署名鍵（ｇ，ｐ，Ｓ1）と、復号鍵（ｇ，ｐ，Ｓ2）との間には、次式の関係をもつ。

$g^{S1} \pmod{p} \equiv T1$

$g^{S2} \pmod{p} \equiv T2$

ただし、ｐは素数である。以下では、ｇ＝４、ｐ＝５、Ｓ1＝２、Ｔ1＝１、Ｓ2＝３、Ｔ2＝４として、説明する。この場合、公開鍵は（４，５，１，４）の組となり、署名鍵は（４，５，２）の組となり、復号鍵は（４，５，３）の組となる。

【００４４】（１）電子署名について

メッセージｍとこのメッセージｍの電子署名の組を（ｍ，Ｘ，Ｔm）とすると、以下の式に示される関係をもつ。

$Tm \equiv g^{R} \pmod{p}$

$dm = MD(m, Tm)$

$X \equiv R + dm \times S1 \pmod{(p-1)}$

ただし、ＭＤ（）は、メッセージダイジェスト関数（ハッシュ関数）であり、ＭＤ（ｍ，Ｔm）は、ｍとＴmを連結したもののハッシュ値である。

【００４５】以下では、説明を簡単にするため、電子署名をするメッセージｍとしてｍ＝３、ＭＤ（ｍ，Ｔm）が３になったと仮定しｄm＝３、乱数ＲとしてＲ＝４を用いるものとする。このとき、

$Tm \equiv g^{R} \pmod{p} = 4^{4} \pmod{5} \equiv 1$

$dm = MD(m, Tm) = 3$

$X \equiv R + dm \times S1 \pmod{(p-1)} \equiv 2$

となり、メッセージとその署名の組は、（３、２、１）となる。

【００４６】この電子署名の確認は、次式が一致することにより行われる。

$g^{X} \pmod{p} = 4^{2} \pmod{5} \equiv 1$

$Tm \times T1^{dm} \pmod{p} = 1 \times 1^{3} \pmod{5} \equiv 1$

上記例では、上記２つの式の値が一致しているので、署名が正当なものであることが確認される。

【００４７】（２）暗号化・復号化について

メッセージｍに対する暗号文（Ｃ1，Ｃ2）は、次式の関係をもつ。

$C1 \equiv g^{R} \pmod{p}$

$C2 \equiv m \times T2^{R} \pmod{p}$

ここでも、説明を簡単にするため、暗号化をするメッセージｍとしてｍ＝３、乱数ＲとしてＲ＝４を用いるものとする。このとき、

$C1 \equiv 4^{4} \pmod{5} \equiv 1$

$C2 \equiv 3 \times 4^{4} \pmod{5} \equiv 3$

となり、メッセージｍ＝３に対する暗号文（Ｃ1，Ｃ2）は、（１，３）となる。

【００４８】この暗号文（Ｃ1，Ｃ2）に対し、復号化は次式で行える。

$m \equiv C2 / (C1^{S2}) \pmod{p}$

$= 3 / (1^{3}) \pmod{5}$

$\equiv 3$

このように、公開鍵（ｇ，ｐ，Ｔ1，Ｔ2）＝（４，５，１，４）用いて暗号化された暗号文は、復号鍵（ｇ，ｐ，Ｓ2）＝（４，５，３）を用いて復号化できる。以上のようにして、１つの公開鍵と、署名鍵と、復号鍵とを生成することができる。

【００４９】次に、公開鍵の実装例について説明する。一般に、公開鍵は、認証局により発行される証明書（デジタル証明書）に含められ利用される。この証明書のフォーマットとして、国際標準であるＩＴＵ－ＴＸ．５０９が利用される。従来のＲＳＡ暗号方式では、公開鍵は

２つの構成要素からなる。例えば、上記実施例１の場合、従来のＲＳＡ暗号方式による公開鍵は、（Ｅ，Ｎ1）の組または（Ｅ，Ｎ2）の組となる。一般に利用されている証明書には、ＲＳＡ暗号方式の場合、２つ構成要素からなる公開鍵がＸ．５０９のフォーマットで格納され利用される（図５（ａ）参照）。

【００５０】一方、本発明に基づく実施例１では、（Ｅ，Ｎ1，Ｎ2）の組で１つの公開鍵を構成している。そこで、本実装例では、Ｘ．５０９ｖ３（バージョン３）において規定される拡張領域（エクステンション・フィールド）を利用し、公開鍵の第２要素Ｎ1または第３要素Ｎ2を、この拡張領域に含めるように実装する。このように実装すると、拡張領域に格納されていない公開鍵のデータは、署名鍵または復号鍵のいずれかに対応する公開鍵として、Ｘ．５０９に対応した既存システムのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）を用いて利用できる。ただし、拡張領域にある公開鍵のデータの一部（Ｎ1またはＮ2）にアクセスするためには、そのための拡張ＡＰＩを別途用意する必要がある。以下に説明する実装例１および実装例２は、実施例１の公開鍵（Ｅ，Ｎ1，Ｎ2）の実装を、このＸ．５０９のフォーマットに適用するものである。

【００５１】［実装例１］本実装例では、Ｘ．５０９ｖ３で規定されている拡張領域を利用して、この拡張領域に公開鍵の第３要素Ｎ2を格納し、公開鍵の第１要素Ｅと署名鍵に対応する第２要素Ｎ1は、基本領域に格納する（図５（ｂ）参照）。この場合、既存ＡＰＩを用いて、拡張領域ではない領域に格納された、公開鍵の第１要素Ｅと署名鍵に対応する第２要素Ｎ1にアクセスできる。したがって、既存ＡＰＩでは、公開鍵と署名鍵を使った暗号化・復号化および電子署名を行える。しかし、既存ＡＰＩによる暗号化を行った場合、署名鍵に対応する公開鍵で暗号化することになるので、署名鍵を紛失した場合、暗号文の復号化が不可能となる。

【００５２】本実装例では、電子署名を、既存ＡＰＩを用いて行い、暗号化は、拡張領域にもアクセス可能な拡張ＡＰＩを別途用意し、基本領域にある公開鍵の第１要素Ｅと拡張領域にある復号鍵に対応する第３要素Ｎ2を用いて暗号化を行う。そして、復号鍵は、別途、鍵管理機関に預託をする。このようにして、復号鍵が紛失しても、この復号鍵は別途預託してあるので、暗号文を復号化できなくなることはない。

【００５３】［実装例２］本方式では、Ｘ．５０９ｖ３で規定されている拡張領域を利用して、この拡張領域に公開鍵の第３要素Ｎ1を格納する（図５（ｃ）参照）。この場合、既存ＡＰＩを用いて、拡張領域ではない領域に格納された、公開鍵の第１要素Ｅと復号鍵に対応する第３要素Ｎ2にアクセスできる。したがって、既存ＡＰＩでは、公開鍵と復号鍵を使った暗号化・復号化および電子署名を行える。そして、復号鍵を、別途鍵管理機関に預託しておけば、この復号鍵が紛失しても暗号文を復号化できなくなることはない。しかし、既存ＡＰＩによる電子署名を行った場合、預託した復号鍵で電子署名をすることになるので、この電子署名に対する事後否認が可能となってしまう。

【００５４】本実装例では、公開鍵による暗号化を、既存ＡＰＩを用いて行い、電子署名は、拡張領域にもアクセス可能な拡張ＡＰＩを別途用意し、基本領域にある公開鍵の第１要素Ｅと拡張領域にある署名鍵に対応する第２要素Ｎ1を用いて、署名鍵を用いてなされた電子署名の確認を行う。こうすることで、電子署名に対する事後否認を防ぐことができる。以上、公開鍵の実装例を説明した。

【００５５】以上では、１つの公開鍵と、署名鍵と、復号鍵からなる３つの鍵を用いているが、署名鍵と復号鍵に対応する公開鍵をそれぞれ用意し、２つの公開鍵と、署名鍵と、復号鍵からなる４つの鍵を用いるようにしてもよい。

【００５６】なお、図１における電子署名部４ｂおよび復号化部４ｃの機能を実現するためのプログラムと公開鍵および署名鍵および復号鍵のデータ、あるいは、鍵生成部４ａ電および電子署名部４ｂおよび復号化部４ｃの機能を実現するためのプログラム、をコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することによりデータセキュリティ装置を実現させてもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【００５７】また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００５８】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録され

ているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００５９】以上、この発明の実施形態を、図面を参照して詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００６０】

【発明の効果】以上、詳細に説明したように、本発明によれば、公開鍵方式による、電子署名に用いる第１の秘密鍵と、暗号文の復号化に用いる第２の秘密鍵を異なるようにしたので、電子署名用の第１の秘密鍵と復号化用の第２の秘密鍵とを別々に管理することができる。したがって、電子署名に用いる第１の秘密鍵を秘密に管理することで、電子署名の事後否認を防止できる。そしてさらに、復号化に用いる第２の秘密鍵を鍵を管理する機関に預託することで、第２の秘密鍵の所有者が自身が所有している第２の秘密鍵を紛失しても、預託した第２の秘密鍵を利用することで、対応する公開鍵で暗号化された暗号文の復号化を行うことができる。また、第１および第２の秘密鍵に対応する公開鍵を共通にしたので、公開鍵の管理を統一的に行える。すなわち、公開鍵を２つ管理する必要がなくなる。また、公開鍵を２つした場合に比べ、公開鍵のデータ長を短くすることができる。

【００６１】また、公開鍵と第１の秘密鍵と第２の秘密鍵をＩＣカード内にもち、公開鍵と第２の秘密鍵を外部に出力し、電子署名用の第１の秘密鍵をＩＣカードから外部に出力しないので、第３者は、ＩＣカードから出力された公開鍵を用いて、ＩＣカード内の第１の秘密鍵でなされた電子署名の確認を行え、また、このＩＣカードが破損ないし紛失しても、外部に出力された第２の秘密＊鍵を用いることで、公開鍵を用いて暗号化された暗号文の復号化が行える。

【００６２】また、公開鍵の電子証明書において、公開鍵の３つの要素の内、第２要素Ｎ1と第３要素Ｎ2の一方を、ＩＴＵ－Ｔ　Ｘ．５０９バージョン３の拡張領域に格納して利用するので、他方の要素と公開鍵の第１要素Ｅは、Ｘ．５０９に対応した既存のシステムでも利用可能となる。

【図面の簡単な説明】

【図１】　本発明の一実施の形態であるデータセキュリティ装置（ＩＣカード）の構成を示すブロック図である。

【図２】　同実施の形態の動作フローチャートの例である。

【図３】　同実施の形態の利用例を示す図である。

【図４】　（ａ）鍵生成／公開鍵の公開／復号鍵の預託を示す図、（ｂ）署名／署名の確認を説明する図、（ｃ）暗号化／復号化／復号鍵の復元を説明する図である。

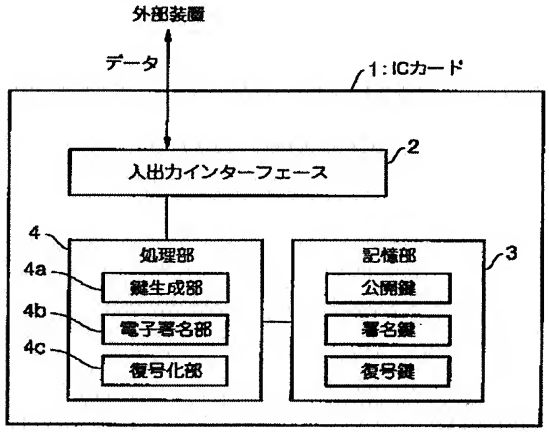
【図５】　（ａ）Ｘ．５０９フォーマットにおける従来の公開鍵の格納形式を説明する図、（ｂ）本発明の一実施の形態の公開鍵の一実装例を説明する図、（ｃ）同実施の形態の公開鍵の他の実装例を説明する図である。

【図６】　従来の公開鍵方式の問題点を説明する図である。

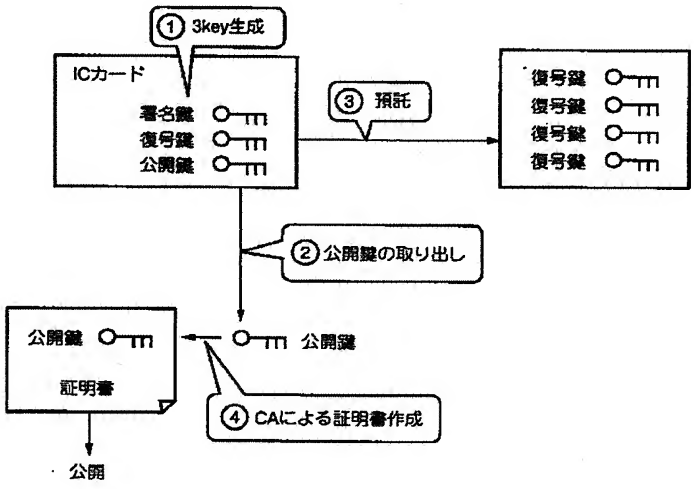
【符号の説明】

１…ＩＣカード（データセキュリティ装置）
２…入出力インターフェース　　３…記憶部
４…処理部　　４ａ…鍵生成部
４ｂ…電子署名部　　４ｃ…復号化部

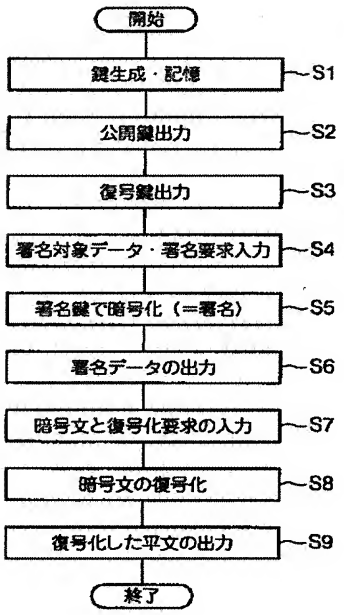
【図１】



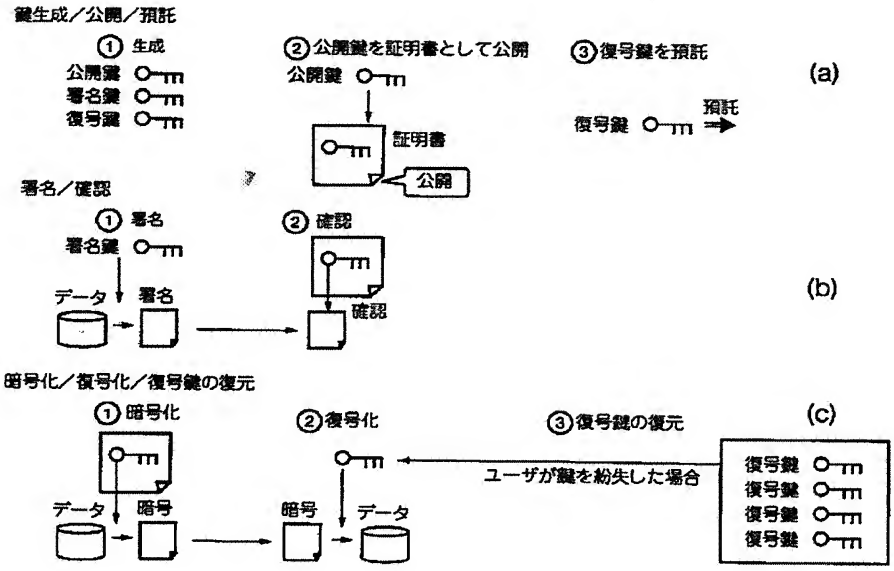
【図３】



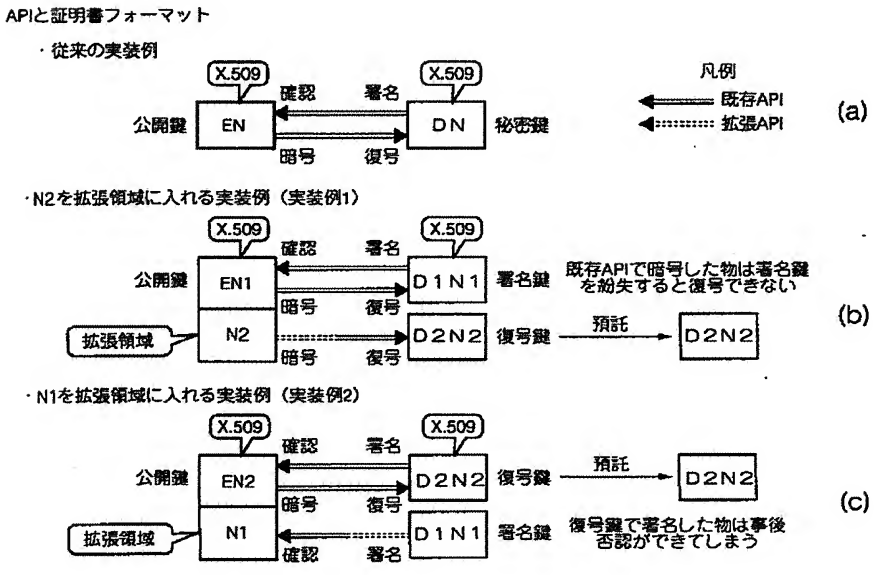
【図２】


開始
鍵生成・記憶
S1
公開鍵出力
S2
復号鍵出力
S3
署名対象データ・署名要求入力
S4
署名鍵で暗号化（＝署名）
S5
署名データの出力
S6
暗号文と復号化要求の入力
S7
暗号文の復号化
S8
復号化した平文の出力
S9
終了

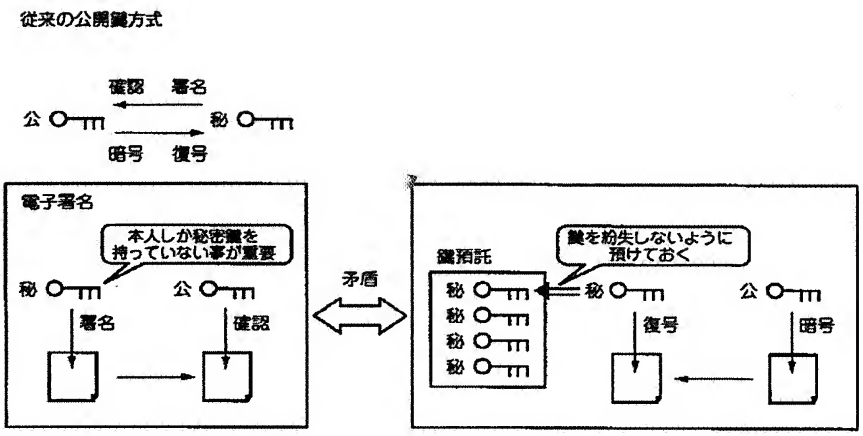
【図４】


鍵生成／公開／預託
① 生成
公開鍵
署名鍵
復号鍵
② 公開鍵を証明書として公開
公開鍵
証明書
公開
③ 復号鍵を預託
復号鍵
預託
(a)
署名／確認
① 署名
署名鍵
データ
署名
② 確認
確認
(b)
暗号化／復号化／復号鍵の復元
① 暗号化
データ
暗号
② 復号化
暗号
データ
③ 復号鍵の復元
ユーザが鍵を紛失した場合
復号鍵
復号鍵
復号鍵
復号鍵
(c)

【図５】


APIと証明書フォーマット
・従来の実装例
X.509
確認
署名
X.509
公開鍵
EN
DN
秘密鍵
暗号
復号
凡例
既存API
拡張API
(a)
・N2を拡張領域に入れる実装例（実装例1）
X.509
確認
署名
X.509
公開鍵
EN1
D1N1
署名鍵
既存APIで暗号した物は署名鍵を紛失すると復号できない
暗号
復号
拡張領域
N2
D2N2
復号鍵
預託
D2N2
暗号
復号
(b)
・N1を拡張領域に入れる実装例（実装例2）
X.509
確認
署名
X.509
公開鍵
EN2
D2N2
復号鍵
預託
D2N2
暗号
復号
拡張領域
N1
D1N1
署名鍵
復号鍵で署名した物は事後否認ができてしまう
確認
署名
(c)

【図６】


従来の公開鍵方式
確認
署名
公
秘
暗号
復号
電子署名
本人しか秘密鍵を
持っていない事が重要
秘
公
署名
確認
矛盾
鍵預託
鍵を紛失しないように
預けておく
秘
秘
秘
秘
秘
公
復号
暗号